

## **Issue 1: Document Structure**

It has been proposed that this Specification be reorganized to more clearly reflect those parts which are specific to the Directory application and those which are more generally applicable. Since the scope of the Specification has expanded it has also been proposed that the reorganization facilitate a clearer grouping of the parts which are relevant to Public-Key Infrastructure and those which are relevant to privilege management. Also to better reflect the current scope of this Specification a title change has been proposed. Following is one proposal for the reorganization and new title. Comments are requested on whether reorganization should or should not be done as well as additional proposals for the reorganization itself. Note that the structure of this PDAM does not assume any reorganization of the standard to which the proposed amendments apply.

**US Position:** Agree

## **Issue 2: Revocation dates**

Revocation date is understood to be the date/time of the first time a revocation notice for a particular certificate published on a CRL. Comments are requested on specific terminology and definitions for the date/time a CA revokes a certificate, the date/time the certificate first appears on a base and or delta CRL etc. In addition comments are requested on whether revocation notices which first appear on delta CRLs should be carried forward to the next base CRL or not. There are at least two situations which are relevant to this issue. A certificate may be revoked and the revocation notice may be first published on a delta CRL. Prior to the issuance of the next base CRL, the certificate may expire. Should this revocation notice be carried forward to the next base CRL? A certificate may be revoked with reason code `certificateOnHold` and first published on a delta CRL. Prior to the issuance of the next base CRL, the hold may be lifted and the certificate listed on another delta CRL with reason code `removeFromCRL`. Should this revocation notice be carried forward to the next issued base CRL?

**US Position:** A revoked certificate that has expired must appear at least once in the base CRL. A certificate that been put on hold and then released during a single CRL issuance cycle, need not appear in the base CRL

## **Issue 3: Roles with public-key certificates**

*It will be difficult to achieve deployment of roles in an environment which only assigns privileges using the `subjectDirectoryAttributes` extension of public-key certificates as this would require a key pair to be associated with a role. Should roles be handled exclusively with attribute certificates? Either a mixed mode environment would be required (assign individuals to roles within public-key certificates and assign the specific privileges to the role within an attribute certificate) or the privileges would be assigned to the role through some means outside the scope of this Specification.*

*The role name must be unique (for example, it may be a Distinguished Name). Some of the options in General Names construct (e.g., IP Address) would be inappropriate for this function.*

*Note: that the use of roles within an authorization framework can increase the complexity of path processing, because such functionality essentially defines another delegation path which must be followed (that is, the delegation path from an AA to the claimant for the role assertion may be (quite) independent of the delegation path from a (possibly separate) AA to the referenced role certificate). The verifier needs to process both paths, ensuring that delegation was done validly at every step. In typical environments, however, it is likely that the delegation path to the role certificate will be relatively short (e.g., it is assigned directly by a Source of Authority), and in such environments the added complexity in path processing would not be significant.*

**US Position:** Disagree. Subject directory attribute is the appropriate location for roles, privileges, and clearances. Given the operational scenario, product costs and other economic factors, the implementers must be provided a mechanism to use the X.509 certificates to convey roles, privileges, authorizations and clearances.

#### **Issue 4: Standardized syntax for policy**

Comments are specifically requested on the usefulness of this optional syntax for privilege policy and whether or not it should be included in this Specification.

**US Position:** The standard should not contain a way to encode privilege (access control) policy. The module has not been validated for accommodating various rule and role based access control policies. The access control policies generally are highly diverse, but simple. Having a single policy syntax makes for a very complex software implementation which may not be as well validated or tested, resulting in security flaws in critical access control decision function

#### **Issue 5: Delegator attribute and Auditability**

It is possible that not all delegators will have certificate issuing software. In those cases, delegators will need to request that an AA issue the delegated attribute certificate. When delegation occurs as a result of a delegation request, the issuer of the attribute certificate does not identify the entity which actually requested the delegation (ie., the entity which currently owns the privilege). Thus, from the point of view of the verifier, the delegation has effectively been blinded.

If this mechanism for requesting delegation is permitted, some mechanism will be required to enable auditability and evidence of delegation which actually occurred.

Should this type of delegation request be permitted or should all delegation be direct and this request to delegate not permitted? If the third party delegation is permitted, does a path validation need to include reference to the owner/delegator? If so, should the following extension be added for this purpose? Note that depending on the outcome of this issue, the delegation path validation process described in 13.13 may need to be updated (ie simplified if third party delegation is not permitted). Note too, that the delegated certificate may also

need to include some evidence that the delegation was requested in the first place (to help protect against rogue AAs).

**US Position:** The standard should not include blinded delegation. There too many unknown here in terms of how the delegation and delegation path will be verified electronically and automatically by verifier software.

#### **Issue 6: Matching on attribute certificate extensions**

The attributeCertificateMatch matching rule probably needs to be more flexible, for example to allow matching on some extension values. Comments are requested on which, if any, extension values should be added as options for this matching rule.

**US Position:** Add the following fields for matching and use matching rules akin to X.509 public key certificate matching rules (attrCertValidityPeriod; authorityAttributeIdentifier; ownerAttributeIdentifier).

#### **Issue 7: CRL Processing normative/informative text**

Some of the content of Annex M includes CRL processing rules which MUST be used at ALL times when CRLs are being processed. Remaining content of Annex M includes description of “one way” to process CRLs, but other methods are also possible. Comments are requested on which sections of this Annex, if any, are mandatory aspects of CRL processing which should be moved into the base standard text. National Bodies are also requested to review this Annex for correctness and consistency with the base standard and identify any required changes.

**US Position:** Most of the text proposed is Normative, specifically section M.3.4.1 through M.3.4.4 and their associated subsections.

#### **Issue 8: Required reason code checking**

Comments are requested on whether the requirement to check CRLs for reason codes key or CA compromise are appropriate or whether a relying party should be required, when following a critical crl distribution points extension in a certificate, to check CRLs covering all the revocation reasons listed in the critical CRL distribution points extension of the certificate. If the reason codes are not listed in the critical CRL distribution points extension of the certificate, should a relying party be required to check CRLs which together cover all revocation reasons?

**US Position:** This is a change in the standard, but a good idea. Applications should be required to check for reason code(s) asserted in critical DP(s). If a critical DP has no reason code asserted, the application should be required to get a CRL that covers all reasons.

## Issue 9: Distribution points and delta CRLs

Comments are requested on whether it is / should be valid to have a situation where a base CRL is not a distribution point CRL, but delta CRLs for that base be published in CRL distribution points. What impact, if any, is there on the delta CRL numbers, the frequency of issue etc. Also, should this text be discussing 'complete' as "complete within the scope of a given certificate" as opposed to "complete for the universe of the CA", especially with respect to CRL distribution points and delta CRLs.

**US Position:** It is Ok to publish only delta CRL via distribution point. It is important that the delta CRL be the one for a base CRL since an authority can publish several delta CRLs for the various base CRL, ARL, and distribution point CRLs. The concern is that the both the base and delta could represent the scope of the certificate in question, but the delta may not be the one for the base the relying party has. Thus, the safest thing to do is to ensure that both the base and the delta are for the scope of the certificate and the delta is for a given base.

While there is no harm in a relying party checking a delta CRL that does not represent a base CRL, absence of a certificate in both the base and delta CRL does not ensure that the certificate has not been revoked prior to the delta CRL issuance and recorded on the delta CRL representing the base.

Rather than complicate CRL processing further and providing warnings rather than a definitive answer, it is recommended that the delta CRLs be used in conjunction with the corresponding base CRLs.

The following is section M.3.4.2 is recommended as replacement.

### M.3.4.2 Validate delta CRL scope

In order to determine that a Delta CRL is appropriate for the certificate, all of the following conditions must hold true:

- Delta CRL indicator extension must be present, and
- The base CRL number in the delta CRL indicator extension should match the base CRL number in the base CRL the relying party has, and
- If the issuing distribution point extension is absent in the base CRL, this extension must be absent from the delta CRL, and
- If the issuing distribution point extension is present in the base CRL, this extension must be present in the delta CRL and must be identical to the one in the base CRL.

## Issue 10: Issuer Name match

Is it acceptable to require that the issue name in a delta must match the issuer name in the base CRL? This makes it impossible for an authority to issue delta CRLs which are indirect and cover multiple base CRLs.

The base CRL identified in the **deltaCRLIndicator** extension must be the most recent base CRL (determined from **nextUpdate** field), and

The relying party must only use the delta CRL in conjunction with the base CRL identified in the **deltaCRLIndicator** extension.

**US Position:** It is ok to issue delta as the indirect. However, as stated in issue 9 above, we recommend that the delta CRLs be used in conjunction with the corresponding base CRL. Thus, if delta indirect CRLs are issued, a base indirect CRL must also be issued. Please note that the current delta CRL syntax does not permit tying a delta CRL to more than one base CRL. Furthermore, the base CRL and the delta CRL must be issued by the same issuer and have the same issuer distribution point values in order to ensure the correspondence.

Please note that section M.3.4.4 does not require the delta CRL to be issued by the certificate issuer only. What it states is that both base and delta CRLs must be issued by the same authority and that either the authority should be the certificate issuer or an indirect CRL issuer asserted in one of the CRL DPs of the subject certificate.

No change is recommended to section M.3.4.4